Money

Inside the World's Biggest Cryptocurrency Hack—and How the Scammers Pulled it Off

By **ROB WILE** January 29, 2018

On Friday, a Japan-based cryptocurrency exchange revealed hackers had stolen more than $500 million-worth of customers' funds in what is thought to be the largest-ever cryptocurrency hack.

It was the latest high-profile crypto hack, and the most significant since $460 million in Bitcoin vanished in 2014. It also comes less than two months after hackers pilfered $70 million from a Bitcoin mining site—a sign that crypto continues to attract hackers.

All hacks are unique, and the most recent one was carried out thanks to security weaknesses at the targeted exchange.

But many are asking why hackers continue to target cryptocurrencies, especially when blockchain technology can record any transaction a user makes—and whether any exchange is truly safe.

Ripe for Thieves

In a hastily called press conference late Friday, the hacked exchange, Coincheck, admitted it had not used adequate security measures to store the stolen cryptocurrency, called XEM. Created by a Singapore-based crypto group called the NEM Foundation, XEM is one of the most popular cryptocurrencies in the world according to Reuters, though remains relatively overlooked in the U.S.

Coincheck said it used different security standards for different currencies, and that unlike customers' Bitcoin holdings, their XEM funds were stored in a "hot wallet"

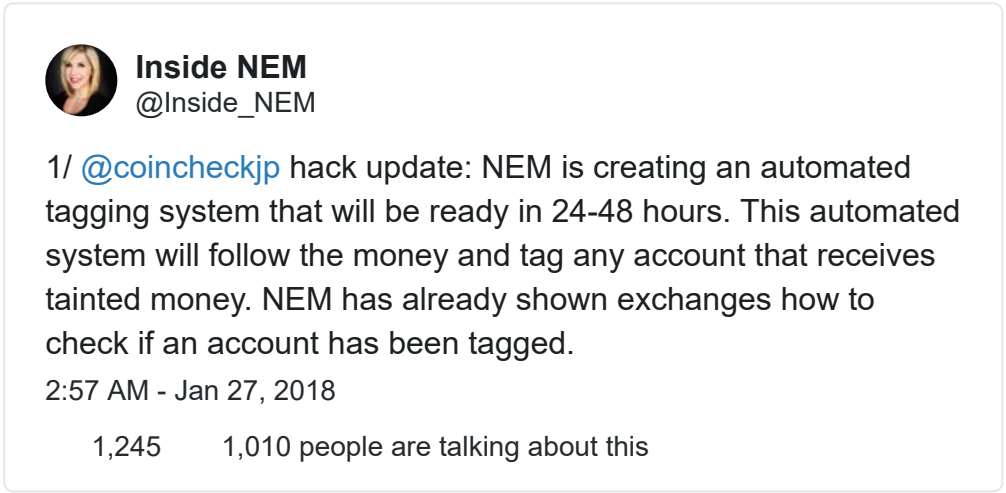
online instead of a "cold wallet" offline—a scenario ripe for hackers.

"Cold storage makes things far safer," Charles Bovaird, who writes extensively about cryptocurrencies for places like *Forbes* and *Investopedia*, told *MONEY*. He noted that Coinbase, one of the largest exchanges in the U.S., holds at least 97% of users' funds in cold storage.

Coincheck also said it did not use multi-signature authentication for its XEM funds, a standard measure for other large-scale holders that requires at least two people for access.

Getting Around Blockchain Tracking

Since XEM revolves around blockchain database technology, the funds can be tracked. And already, Coincheck has found the 11 addresses where all 523 million of the stolen coins ended up. The addresses have been labeled by XEM developers with a tag that reads "coincheck_stolen_funds_do_not_accept_trades : owner_of_this_account_is_hacker." The developers have also created a tracking tool that allows exchanges to automatically reject those stolen funds.



But as *Bloomberg* notes, the hackers are still likely to be able to use the funds. Some sites provide a service called a "tumbler" that offers cryptocurrency trading without collecting personal data, the crypto equivalent of laundering money.

The huge sum of money stolen is a major challenge, *Bloomberg* continues. It would take awhile to spend down all the funds and at least one major tumbler serviced has banned usage of the stolen cryptocurrency.

Are All Exchanges Vulnerable?

Bovaird says it is safe to question whether any large-scale holder of cryptocurrency is truly immune from hacking or attack, though he did note that Coinbase has yet to be successfully infiltrated.

“Centralization of resources—I think of it as a big carrot dangling in front of criminals that’s covered with money,” he said.

Even Bitfinex, a popular exchange that did use multi-factor authentication, experienced a high-profile hack, he noted, which led some to question whether the hack was an inside job.

“I think people want to keep those facts in mind,” he said.

But XEM users look like they dodged a bullet. Coincheck has promised to reimburse nearly 90% of the losses.